

天翼云 • 主子账号及权限管理 用户使用指南

中国电信股份有限公司云计算分公司



目 录

1	概述	
1.1	产品定义	
1.2	术语解释	
1.3	应用场景	
1.4	产品功能	
1.5	开通方式	5
2	快速入门	5
2.1	创建用户组	5
2.2	子用户分组	7
2.3	创建企业项目	9
2.4	迁入资源	
2.5	分配用户组	
3	其他操作	
3.1	策略管理	
3.1.1	策略语言说明	
3.1.2	? 创建自定义策略	
3.2	企业项目管理	
3.2.1	! 修改/启用/停用企业项目	
3.2.2	? 新购云资源选择企业项目	
		1



3.2.3	迁出资源	
3.2.4	移除用户组	
4 常	见问题	
4.1	在什么场景下可以看到所有的企业项目	
4.2	为什么在企业项目管理侧为子账号设置了 EPS ADMIN 的策略,	但该账号不具备添加用户组及设置策
略的权	限	
4.3	如何获取企业项目 ID	

目录

1 概述

1.1 产品定义

主子账号及权限管理:借助企业项目服务为多用户共同使用天翼云账号,匹配对应权限,进行访问 控制,实现多层级组织和项目结构相匹配的天翼云资源管理提供平台能力支持。

1.2 术语解释

主账号:用户在天翼云注册后自动创建,该账号对其所拥有的资源具有完全的访问权限,可以重置 用户密码、分配用户权限等。如果需要多人共同使用天翼云资源,由于账号是付费主体为了确保账 号安全,建议创建子用户来进行日常管理工作。

子账号:由主账号在用户中心创建的账号,子账号的用户名、密码统一由主账号创建管理。子账号 同样可以登录访问天翼云控制台,登录入口与主账号相同,受主账号赋予的权限限制。

策略:是描述一组权限集的语言,它可以精确地描述被授权的资源集和操作集,通过策略,用户可 以自由搭配需要授予的权限集。通过给用户组授予策略,用户组中的用户就能获得策略中定义的权 限。

系统策略:系统预置的常用权限集,主要针对不同云服务的只读权限或管理员权限,比如对 ECS 的 只读权限、对 ECS 的管理员权限等;系统策略只能用于授权,不能编辑和修改。

自定义策略:由用户自己创建和管理的权限集,是对系统策略的扩展和补充。

企业项目:将云资源、企业成员按项目进行管理,通过企业项目将云资源、带有权限的用户组绑定 到一起,用户使用项目内云资源的权限受用户组的授权限制。

1.3 应用场景

企业可以根据组织架构规划企业项目,每个企业项目配置独立的云资源,同时为每个企业项目设置 不同的用户组。管理员用户可以管理所有的企业项目及资源。



企业管理应用场景

1.4 产品功能

主子账号管理

天翼云用户可以创建多个账号,供多人共同管理和使用天翼云平台的资源。为用户分配不同的用户 组。

策略管理

通过制定策略实现云资源操作权限的管理,天翼云为用户提供了制定好的策略即系统策略,用户也可以自定策略。例如,ECS的开机、关机、重启、更换操作系统等或只读。将策略赋予用户组,实现 组内用户具备完成职责所需的最小操作权限。

用户组授权

无需为每个用户进行单独的授权,只需规划用户组,并将对应权限授予用户组,然后将用户添加至 用户组中,用户就继承了用户组的权限。如果用户权限变更,只需在用户组中删除用户或将用户添 加进其他用户组,实现快捷的用户授权。

资源管理

将资源迁入项目,相当于为资源打项目标签,并不影响资源的位置。

企业项目管理

将项目成员以用户组方式与企业项目绑定,实现用户在用户组细粒度权限限制下使用项目资源。

1.5 开通方式

当前采用公测的方式上线能力,用户有使用需求请联系天翼云开放能力操作界面。

2 快速入门

2.1创建用户组

 1、登录天翼云账号在【管理中心】点击右上角头像,在下拉列表中找到"用户组管理"。或者点击 左上角头像,进入个人中心页面,在左侧导航栏中找到"用户组管理"。





2、点击【添加】,填写用户组信息。

个人中心	用户组名称:	搜索 添加	
基本信息	用户组名称	用户组描述	操作
修改资料	ceshi	企业项目测试	查看编辑删除
身份认证	admin1	最高权限组	查看编辑删除
更换手机	安全jpv6	用于测试安全产品的ipv6功能	查看编辑删除
用户组管理	GZTX	广州特训	查看编辑删除
子用户管理	SSLVPN	ipv6测试	查看编辑删除
	viewer	只读组	查看编辑删除
	A	华南	查看编辑删除
	В	华北	查看编辑删除
	Lfipv6	服务器安全卫士ipv6测试	查看编辑删除
			共9条 10条/页 ∨ < 1 > 前往 1 页

		搜索	添加	
添加用户组				×
* 用户组名称:				
* 用户组描述:				
				.:
			取消	确认
		l		
	口法妇			

用户组列表在用户组管理页面、统一身份认证的用户页面、企业项目管理的用户页面同步。

3、点击【查看】进入到子用户管理页面。

4、点击【编辑】可以对组名称和描述进行修改。删除用户组需要先将组内用户移除。

修改用户组		×
* 用户组名称:	admin1	
* 用户组描述:	最高权限组	
		取消 确认

2.2子用户分组

 1、登录天翼云账号在【管理中心】点击右上角头像,在下拉列表中找到"子用户管理"。或者点击 左上角头像,进入个人中心页面,在左侧导航栏中找到"子用户管理"。



个人中心	基本信息
基本信息	
修改资料	
身份认证	
修改密码	
更换手机	更换头像
用户组管理	
子用户管理	安全验证
	登录密码:

2、点击【添加】,填写用户信息,选择用户所在用户组。

添加子用户		×
* 用户组:	ceshi ~	
* 邮箱:]
* 用户名:)
* 手机号:		
*原密码:)
* 确认密码:)
	取消 确论	

创建完成的用户与天翼云账号登录地址相同,用户列表在子用户管理页面、统一身份认证的用户页面、 企业项目管理的用户页面同步。

2.3创建企业项目

1、在头像下拉菜单点击"企业管理"进入企业项目管理页面,选择"企业项目管理",

💮 xiaobo@c 🔺
用户中心
我的订单
消费详情
我的凭证
企业管理
切换角色
提交工单
备案中心
退出

单击【创建】,弹出"创建企业项目"页面。





输入名称和描述,单击"确定"。

🛄 说明

- 名称不能为空。
- 名称不超过 64 个字符,只能由中文、英文字母、数字、下划线、中划线组成,且不能使用任何大 小写形式的"default"。
- 描述不超过 512 个字符。

2.4迁入资源

企业项目管理提供统一的云资源按企业项目管理,用户可通过企业项目管理服务对企业项目内的资 源进行查看、迁入和迁出操作。

目前支持的资源如下:

企业项目当前支持的资源

产品类型	资源类型
弹性云主机(ECS)	弹性云主机(Elastic Cloud Server)
弹性伸缩(AS)	弹性伸缩组(Auto Scaling)
云硬盘(EVS)	磁盘(Disk)
弹性公网 IP(EIP)	弹性公网 IP(Elastic IP)
虚拟私有云(VPC)	虚拟私有云(Virtual Private Cloud)
	六字市见 (Shareu Bandwidth)

产品类型	资源类型
	安全组(Security Group)
镜像服务(IMS)	私有镜像(Private Image)

在企业管理页面,选择"企业项目管理"。选择待查看的企业项目,单击操作列【查看资源】。 进入企业项目详情页面,如下图,

E	企业项目管理 ,演示项目		新购资源 停用 C		
<u>]-]</u>] 企业管理	名称 演示项目 状态 ◆ 已启用	ID 8d4da6b3-a954-4d2 创建时间 2019-03-08 16:26:16	1-a096-0b90edb6b7db GMT+08:00		
企业项目管理	描述	修改时间 2019-03-08 16:26:16	GMT+08:00		
人员管理	资源 用户组				
	产品类型 全部 ECS AS IMS	EVS VPC Bandwidth EI)		
	近入 近出		请输入资源名称 Q C		
	资源名称	所属区域 产品类型	资源类型		
	ecs-9b29 258014fd-0fb6-4b1a-ac05-5aa1cc831d5b	贵州 EVS	磁盘		

在"资源"页签下可查看该企业项目内资源信息。默认展示全部区域及全部产品类型的资源信息,可进 行资源筛选。

设置资源搜索条件。

- 1、 设置搜索区域。
- 2、设置产品类型。
 系统默认选中"全部",根据需求选中产品类型,下方可进一步对资源类型进行 选择。
- 3、 输入资源名称。

页面下方列表展示筛选后的所有资源。

迁入资源步骤如下,

在企业管理页面,选择"企业项目管理"。选择待查看的企业项目,单击操作列【查看资源】。

进入企业项目详情页面,在"资源"页签下可查看该企业项目内资源信息。

- 1、单击【迁入】,弹出"迁入资源"页面。
- 2、选择待迁入资源所在的"企业项目",下方展示该企业项目下的所有资源。
- 3、单击 7,对"所属区域"或"产品类型"进行筛选。下方展示符合条件的资源。

ていた を Cloud ・ 控制	迁入资源				× 🚱 xiaobo@c ▼ ⊠ ? ^
	 单资源迁入支持不同资源同时; 关联迁入仅支持ECS及其关联; 	单资源迁入支持不同资源同时迁入,其中已关联ECS的EVS、EIP只支持迁入到该关联ECS所在企业项目;ECS 关联迁入仅支持ECS及其关联资源EVS、EIP同时迁入。			▲ 新购资源 停用 C
企业管理	迁入方式 单资源迁入	ECS关联迁入			196-0b90edb6b7db
企业项目管理	资源所在企业项目 default	~		请输入资源名称 Q	T+08:00 T+08:00
人员管理 🎽	资源名称	所属区域 🏹	产品类型 🔽	资源类型	
	volume-ecda 贵州 EVS 磁盘 mirror_test 贵州 IMS 私有镜像 chens_test 贵州 IMS 私有镜像 ceshi_jngxinag 贵州 IMS 私有镜像	磁盘			
		私有镜像			
		私有镜像			
		私有镜像			
	wl_create_img_test0	贵州	IMS	私有镜像	
	qiuyang	贵州	IMS	私有镜像	请输入资源名称 Q C
	qiuyang	贵州	AS	弹性伸缩组	
	444444444444444444444444444444444444444	贵州	VPC	安全组	資源夫型
	Sys-default	贵州	VPC	安全组	磁盘
④ 中文(简体)	sq-6cc7	贵州	VPC	安全组	0001 天翼云首页 用户协议 法律声明

迁入资源

🛄 说明

迁入操作暂不支持关联操作,如迁入 ECS 不会同时迁入绑定的 EIP、EVS 等,如需迁入关联的资源,请选择关联的资源一同迁入。

4、勾选待迁入资源,单击操作,如迁入 ECS 不会同时迁入绑定的 EIP、EVS 等,如需迁入关联的资

2.5分配用户组

用户组中的用户具备对应企业项目的权限,当企业项目权限有变动时,可对企业项目中的用户组进 行添加、移除操作,使企业项目管理更加高效灵活。

在企业管理页面,选择"企业项目管理"。选择待查看的企业项目,单击操作列【查看用户组】。 进入企业项目详情页面,如下图,

	控制	中心 服务列表 ▼ 收藏 ▼						() xiaobo@c 🔹		?
E		企业项目管理 ,演示项目							新购资源	停用	C
企业管理		名称 演示项目				ID	8d4da6l	b3-a954-4d24-a096-0b	90edb6b7db		
企业项目管理		状态 📀 已启用				创建时间	2019-03	-08 16:26:16 GMT+08:0	00		
人员管理	~	油述				修改时间	2019-03	-08 16:26:16 GMT+08:0	0		
		资源 用户组									
		添加用户组 批量移除									C
		用户组名称	用户数量	关联策略(该	描述			添加时间	操作		
		zhan	1	2	zhanpeitest			2019-03-08 16:42:	设置策略 移除		
		©20	19中国电信股份有	限公司云计算分公司期	版权所有 京ICP备 12	2022551号 増値時	电信业务经营	许可证A2.B1.B2-20090001	│ 天翼云首页 │ 用	⇒协议 ½	建声明

此处的添加用户组是将已有用户组添加到所选项目的操作。操作如下,

在企业管理页面,选择"企业项目管理"。选择待查看的企业项目,单击操作列【查看用户组】。 进入企业项目详情页面,在"用户组"页签下可查看该企业项目用户组信息。

1、单击【添加用户组】,弹出"添加用户组"页面,如下图。

		× 《 xiaobo@c ▼ 区 新购资源 停用
企业管理	可选用户组 请输入用户组名称 Q 已选用户组 请输入用户	P组名称 Q
	用户组名称/描述 用户组名称/描述	0b90edb6b7db
2业项目管理	admin	18:00
(员管理 ~	adminGroupDes	18:00
	EVS_test >>	
	test1 《 无记录	
	xz666	操作
	X	设置策略 移除
	test v	
	您还可以选择10个用户组	
∂中文(简体)	T-11- 8734)1 天興云首页 用户协议 ;

添加用户组

- 2、(可选)查询可选用户组。在"可选用户组"展示框中展示用户组过多时,可在输入框中输入待添加用 户组,进行查询。
 - 3、勾选待添加用户组,单击 >>> 即可将待添加的用户组同步至"已选用户组"展示框。
 - 4、单击"下一步",对新添加的用户组设置策略,使该用户组在所属企业项目中拥有策略定义的权限。

	用户组名称 EVS			👩 xiaobo@c 🔻 🛛
001044	可选策略	创建自定义策略 C	已选策略	
-E	所有策略 ▼ 请输入	_{衰略名称} Q	所有策略 ▼ 请输入策略名称 Q	新购资源 停用
<u> - </u>	策略名称/策略描述	类型	策略名称/策略描述 类型	
企业管理	ECS User	系统策略		
企业项目管理	IMS Viewer 镜像服务查看权限	系统策略	»	0690edb6b7db
人员管理 💙	Full Access 所有服务的所有权限	系统策略	《 ————————————————————————————————————	18.00
	EVS Viewer	系统策略	Juca	
	ECS Viewer	系统策略		
	EVS Admin	系统策略		操作
	NDC Adarta	<i>▼:1→-htmb</i> ¥		
	您还可以选择25个策略			
	∨ 策略内容			
❷ 中文 (简体)		上一步	柳定	1 天翼云首页 用户协议

5、选择策略。您可以在可选策略的下拉复合框中按照"所有策略""自定义策略""系统策略"对已有 策略进行筛选,也可以创建自定义策略。

	 用户组名称 EVS 可选策略 所有策略 ▼ 请输入第 所有策略 		 ご ご<th></th>	
企业管理	自定义策略 系统策略	系统策略	来自日初以来自用应 大士	0b90edb6b7db
企业项目管理	镜像服务查看权限	系统策略		18:00
人员管理 >	Full Access 所有服务的所有权限	系统策略	しリ 无记录	
	EVS Viewer	系统策略		
	ECS Viewer	系统策略		
	EVS Admin	系统策略		操作
		VDC A J1		设置策略 移除
	您还可以选择25个策略✓ 策略内容			
④ 中文(简体)		上一步 确定	取消	01 天興云首页 用户协议

选择策略

创建自定义策略的具体操作请参见 3.1.2<u>创建自定义策略</u>。企业项目可选系统策略及对应含义见下表, 平台支持策略查看附件 1。

服务名称	权限名称	权限说明	适用的典型人员
BASE	Full Access	对账号拥有的所有云资源的所有执行权限。	

弹性云主机	ECS Admin	ECS 的管理员权限,拥有该权限的用户拥有 ECS 的全部权限,包括	企业资产管理员
(ECS)		创建、删除、查询、变更规格等操作。	
	ECS User	ECS 的普通用户权限,拥有该权限的用户可以执行查询、重启等通	虚拟机使用人员
		用操作,不能执行创建、删除、重装/切换操作系统、变更规格等	
		高级操作。	
	ECS Viewer	ECS 的只读权限,拥有该权限的用户可以执行查询操作,例如查询	企业资产查询人
		云服务器列表。	员、非虚拟机使用
			人员
虚拟私有云	VPC Admin	VPC 的管理员权限,拥有该权限的用户拥有 VPC 下所有资源的所有	企业资产管理员
(VPC)		操作权限,包括创建、删除、修改、查看等操作。	
	VPC Viewer	VPC 的只读权限,拥有该权限的用户可以执行查询操作,例如查询	企业资产查询人
		虚拟私有云、子网、安全组、弹性 IP 等。	员、非网络业务使
			用人员
云硬盘	EVS Admin	EVS 的管理员权限,拥有该权限的用户拥有 EVS 的所有操作权限,	企业资产管理员
(EVS)		包括创建、删除、修改、查看操作等。	
	EVS Viewer	EVS 的只读权限,拥有该权限的用户可以执行查询操作。	企业资产查看者
专属云独享存	DSS Admin	对独享存储服务的所有执行权限。	企业资产管理员
储(DSS)	DSS Viewer	对独享存储服务的只读权限。	企业资产查看者

6、单击 , 将选择的策略同步至"已选策略"展示框。

7、单击"确定",用户组添加完成。在当前企业项目的用户组列表中即可查看添加的用户组信息。

٠	添加用户组时,每次最多可添加10个。
•	设置策略时,每个企业项目对应的用户组最多可以选择25个策略。
•	策略生效时间大约需要 30s, 您可以选择重新登录进行查看。

其他操作

若需要为该企业项目下已有的用户组设置策略时,可单击该用户组右侧操作列的"设置策略",如 下图。具体设置方式请参见上述步骤 5。

	控制	J 中心 服务列表 ▼ 收藏 ▼						💮 xiaobo@c 🔻	⊠ ?
		企业项目管理, 演示项目						新购资源	明 C
企业管理		名称 演示项目				ID	8d4da6b3-a954-4d24-a096-0	b90edb6b7db	
企业项目管理		状态 😏 已启用				创建时间	2019-03-08 16:26:16 GMT+08	:00	
企业项目管理 人员管理 ~	~	 描述 资源 用户组 添加用户组 批量移除 				修改时间	2019-03-08 16:26:16 GMT+08	:00	С
		用户组名称	用户数量	关联策略(该…	描述		添加时间	操作	
		zhan	1	2	zhanpeitest		2019-03-08 16:42:	设置策略移除	



3.1策略管理

1、顶部导航栏找到"操作列表",然后找到"统一身份认证",点击进入。

で た デ デ デ デ ご ・	收藏▼			💮 xiaobo@c 🔻 🗌	⊠ ?
计算		存储		网络	^
弹性云主机	•	云硬盘	•	虚拟私有云	•
云容器引擎		专属存储		弹性负载均衡	•
物理机服务	•	云主机备份		VPN	
镜像服务	•	云硬盘备份	•	云解析服务	
函数工作流 FunctionGraph		对象存储服务		NAT网关	
弹性伸缩服务				弹性公网IP	
专属云					
安全		管理与部署		应用服务	
Web应用防火墙	•	云监控服务		分布式消息服务	
Anti-DDoS		云审计服务		应用性能管理	
Anti-DDoS流星清洗		统一身份认证服务	\heartsuit	应用运维管理	
Web应用防火墙[旗舰版]		统一身份认证服务		技术服务	
数据库安全服务				域名服务	
数据加密服务					

2、在统一身份认证控制台可以找到策略。

	22制中心 服务列表 ▼ 收藏 ▼			💮 xiaobo@c 🔻 🗏 🗹 📍
L=	策略 ②			+ 创建自定义策略
统一身份认证服务				
	您还可以创建116个自定义策略。			全部类型 ▼ 请输入策略名称。 Q
用户	策略名称 ↓	策略类型 💲	策略描述 💲	操作
用户组	evs_types	自定义策略		编辑册除
策略	EVS_Admin	自定义策略		编辑 删除
委托	ECS_test	自定义策略		编辑 删除
身份提供商	xz_test	自定义策略	test	编辑 删除
账号设置 >	EVS_Viewer	自定义策略		编辑 删除
	allow_all	自定义策略		编辑 删除
	aslist	自定义策略		编辑 删除
	nyc_first_cl	自定义策略	no1	编辑 删除

天翼云平台有以下两种形式的策略:系统策略和自定义策略。

3.1.1 策略语言说明

策略结构

细粒度授权策略结构包括策略版本号(Version)及策略授权语句(Statement)列表。

- 策略版本号: Version, 标识策略结构的版本号。
- 1.0: 非细粒度权限。
- 1.1: 细粒度权限。
 - 策略授权语句: Statement,包括了基本元素:作用(Effect)和权限集 (Action)。

策略结构模型



策略基本元素

策略授权语句(Statement)描述的是策略的详细信息,包含作用(Effect)和授权项(Action)。

● 作用(Effect)

作用包含两种:允许(Allow)和拒绝(Deny),当策略中既有 Allow 又有 Deny 的授权语句时,遵循 Deny 优先的原则。

授权项(Action)
 对资源的具体操作权限,支持单个或多个操作权限。
 格式为:服务名:资源类型:操作,例如:vpc:ports:create。

🛄 说明

{

• 服务名:产品名称,例如 ecs、evs 和 vpc 等,服务名仅支持小写。

• 资源类型和操作没有大小写要求,支持通配符号*,用户不需要罗列全部授权项,通过配置通配符号*可以方便快捷地实现授权。

策略样例

• 支持单个操作权限,例如:查询弹性云主机详情权限

```
"Version": "1.1",
"Statement": [
{
"Effect": "Allow",
"Action": [
```

```
"ecs:servers:list",
                           "ecs:servers:get",
                           "ecs:serverVolumes:use",
                           "ecs:diskConfigs:use",
                           "ecs:securityGroups:use",
                           "ecs:serverKeypairs:get",
                           "vpc:securityGroups:list",
                           "vpc:securityGroups:get",
                           "vpc:securityGroupRules:get",
                           "vpc:networks:get",
                           "vpc:subnets:get",
                           "vpc:ports:get",
                           "vpc:routers:get"
                     1
               }
         ]
   }
   支持多个操作权限,例如:锁定云服务器和创建云硬盘权限。
    {
        "Version": "1.1",
         "Statement": [
               {
                     "Effect": "Allow",
                     "Action": [
                           "ecs:servers:lock",
                           "evs:volumes:create"
                     ]
               }
         ]
   通配符号*用法示例:对 ECS 服务资源的 Tenant Guest 权限。
🛄 说明
   ECS 服务的 Tenant Guest 权限需要依赖 EVS、VPC、IMS 服务的 Tenant Guest 权
   限。
   {
       "Version": "1.1",
       "Statement": [
           {
               "Effect": "Allow",
               "Action": [
                  "ecs:*:get",
                  "ecs:*:list",
                  "ecs:serverGroups:manage",
                   "evs:*:get",
                   "evs:*:list",
                   "vpc:*:get",
```

```
"vpc:*:list",
"ims:*:get",
"ims:*:list"
]
}
]
```

策略语法

策略结构体不完整时,将不能通过系统的语法校验。

}

```
Policy = \{
<version block>,
<statement block>
}
<version block> = "Version" : "1.1"
<statement_block> = "Statement": [<statement>, <statement>, ...]
<statement> = {
<effect block>,
<action_block>
<effect block> = "Effect" : ("Allow" | "Deny")
<action_block> = "Action": ("*" | [<action_string>, <action_string>, ...])
   策略中[]字符为允许多值的意思,当一个元素允许多值时,使用逗号和省略号来
   表达, 比如[<statement>, <statement>, …], [<action_string>,
   <action_string>, …]。
   多值之间如果用竖线 ()) 隔开, 表示取值只能选取这些值中的一个。比如:
   ("Allow" | "Deny")。
   当元素取值为数字时,与字符串类似,需要用双引号括起来。比如:
   <version block> = "Version" : "1.1"。
```

 当元素取值为字符串(String)时,支持(*)模糊匹配来代表 0 个或多个任意 的英文字母。

您还可以通过以下网站了解更多有关 JSON 的语法标准:

https://tools.ietf.org/html/rfc7159?spm=a2c4g.11186623.2.12.M8YmXV

检查规则

用户被授予的访问策略中可以包含多个授权语句,当策略中既有 Allow 又有 Deny 的授权语句时,遵

循 Deny 优先的原则。

用户访问资源时,权限检查逻辑如下:



说明 每条策略做评估时, Action 之间是或(or)的关系。

- 1. 用户发起操作请求,鉴权开始。
- 在用户被授予的访问策略中,系统将优先寻找显式拒绝指令。如找到一个适用的 显式拒绝,系统将返回 Deny 决定,鉴权结束。
- 3. 如果没有找到显式拒绝指令,系统将寻找适用于请求的任何 Allow 指令。

如找到一个显式允许指令,系统将返回 Allow 决定,由服务继续处理该请求。 如果找不到显式允许,最终决定为 Deny。

4. 如果代码在评估过程中的任意点遇到错误,它将生成异常并关闭。

3.1.2 创建自定义策略

系统预置的权限不能满足要求时,您可以创建自定义策略,并通过给用户组授予自定义策略来进行 精细的访问控制。

1、在服务列表,选择"管理与部署 > 统一身份认证服务"。在左侧导航窗格中,单击"策略"。 在"策略"界面,单击"创建自定义策略"。

	控制中心 服务列表 ▼ 收職 ▼	⊢⊠?
	策略,创建自定义策略	
统一身份认证服务	基本信息	
用户	*策略名称	
用户组		
策略		
委托	策略描述 请输入策略描述。	
身份提供商		
账号设置 >	0/255	
	策略信息 选择模板 校验语法	

2、输入"策略名称"。选择"作用范围"。

- 全局级服务: 生效范围为全局, 该策略在所有区域都生效。
- 项目级服务:策略生效的范围为各区域中的项目,该策略仅在授权项目中生效, 如果需要对多个项目生效,需要分别对多个项目进行授权。

例如: 创建云硬盘的细粒度策略("evs:volumes:create"),由于 EVS 服务属于项目级服务,作用 范围必须选择项目级服务,如果需要该策略对多个项目生效,需要对多个项目分别授权。

3、(可选)输入"策略描述"。

在"策略信息"区域,单击"选择模板",例如选择"VPC Admin"作为模板。

入 Recloud ・	控制中心 基本作	选择模板		×	🎯 xiaobo@c 🔻 🗹 ?	Î
L≡	*策略:	全部模板 ▼ 请输入模板名称 Q	{ "Version": "1.1",			
一身份认证服务	*作用:	BASIC	"Statement": [{			
	Andre materia	Full Access	"Effect": "Allow", "Action": [
7	東南	EVS	"vpc:*:*",			
组		EVS Viewer	ecs:*:list*"			
ŝ		EVS Admin	}			
6		VPC]			
いたので	策略信	VPC Admin				
	洗择	VPC Viewer				
设置		DSS				ľ
		DSS Admin				
		DSS Viewer				
		CUSTOMED				
中文(简体)		evs_types v			B2-20090001 天興云首页 用户协议 法律声明	, .

4、单击"确定"。

修改模板中策略授权语句(Statement)中的作用(Effect)和权限集(Action)。

🛄 说明

- 自定义策略版本号(Version)固定为1.1,不可修改。
- 自定义策略中可以包含多个策略授权语句(Statement)。
 - 作用(Effect): 允许(Allow)和拒绝(Deny),当策略中既有 Allow 又有 Deny 的授权语句时,遵循 Deny 优先的原则。
 - 权限集(Action): 写入各服务 API 授权项列表中"授权项"中的内容,例如: "vpc:vpcs:create",来调用表格左侧的"API",实现"API 功能"支持的细粒度 授权。

授权项示例

API	API功能	授权项
POST /v1/{tenant_id}/vpcs	创建VPC	vpc:vpcs:create

5、单击"确定"。

🛄 说明	
如果系统提示语法错误,	请按照语法规范进行修改。

自定义策略创建成功。用户可以在用户组中选择新创建的自定义策略,实现细粒度授权。

后续操作

- 修改自定义策略
 当用户的权限发生变更时,您可以修改自定义策略。
 单击自定义策略页签中,目标策略"操作"列的"修改",修改自定义策略的名称、描述及策略信息。
- 删除自定义策略
 当您不再需要自定义授权策略时,您可以将自定义策略删除。
 单击自定义策略页签中,目标策略"操作"列的"删除",删除自定义策略。
- 将新创建的自定义策略授权给用户组,使用户组中的用户具有策略定义的权限
 a. 单击目标用户组"操作"列的"修改"。
 - b. 在"用户组权限"区域中,单击需要授权项目"操作"列的"修改"。
 - c. 在"策略"对话框中的"可选择策略"区域选择新创建的自定义策略。

3.2企业项目管理

3.2.1 修改/启用/停用企业项目

修改企业项目

在企业管理页面,选择"企业项目管理"。选择待修改企业项目,单击操作列【修改】。弹出"修 改企业项目"页面。修改"名称"或"描述"。单击"确定",完成修改。

企业项目管理								
企业项目管理 <mark>I</mark>)、云硬盘(EV:	修改企	È业项目			×	云服	务器(ECS)	. 3
	* 名称	test1						
创建您还	1444 10					1	请输入	入企
名称	油述						操作	
default							查看资源	重
test1				0/512			查看资源	査
演示项目			_				查看资源	直
1111111			确定	取消			查看资源	蔖
pppp	Ə E	已启用		2019-02-15 15:01:	2019-02-23 16:22	:	查看资源	重

- 🛄 说明
- 名称不能为空。
- 名称不超过 64 个字符,只能由中文、英文字母、数字、下划线、中划线组成,且不能使用任何大小写形式的"default"。
- 描述不超过 512 个字符。

停用企业项目

在企业管理页面,选择"企业项目管理"。选择状态为已启用的企业项目,单击操作列"更多 > 停 用"。弹出"停用企业项目"确认页面。单击"停用"。

1		2010 02 00 16-42-	2010 02 09 16:4	3: 查看资源
项目	停用企业项目		× :2	6: 查看资源
1111	▲ 确定更信田 "vz te	sct2" 吗?	:4	1: 查看资源
q	停用后该企业项目在云服	资中将不可见,无法迁入资源和	1添加用户 :2.	2: 查看资源
est	组,且资源仍然继续计费	度,如需再次使用,请重新启用证	《企业项目。 :3〕	7: 查看资源
intext02			:3	3: 查看资源
_test666	停用	取消	:0	0: 查看资源
erprise_project1	● 已启用 描述	2019-01-14 17:22:	2019-01-14 17:2	2: 查看资源
est2	∂ 已启用	2019-01-11 11:54:	2019-01-11 11:5	4: 查看资源
▼ 总条数:14	< 1 2 >			

启用企业项目

在企业管理页面,选择"企业项目管理"。选择状态为已停用的企业项目,单击操作列"更多 > 启 用"。

🛄 说明

- 已停用企业项目无法使用修改功能。
- 企业项目停用后在云服务中将不可见,无法迁入资源和添加用户组,如需再次使用,请重新启用 该企业项目。

当未完成的订单包含该企业项目时,需完成订单后才可停用该企业项目。未完成的订单状态包括:待支付、处理中、待审核、待审批。

默认企业项目无法编辑和停用。

3.2.2 新购云资源选择企业项目

在购买云资源页面,您可以选择已启用的企业项目,新购云资源将可按此企业项目进行管理。

以弹性云主机为例,在购买弹性云主机页面,进行如下配置:

- 高级配置:"现在配置"。
- 企业项目:在下拉列表中选择目标企业项目。

[]	
高级配置	暂不配置 现在配置
用户数据注入	文本 文件 如何注入?
	用户数据内容
云服务器组 🕐	请选择 ▼ 查看云服务器组 C
企业项目 🕜	default - C
标签	Q ETMS创建全局的预定义标签,再进行标签与资源的关联操作。 查看预定义标签
	default 值
	企业创新项目 请输入标签值
	您还可以增加10个标签
代理名称 🧿	请选择- ▼ 查看代理名称 C

选择企业项目

🛄 说明

• 默认企业项目为 default, 后续若要按其他企业项目进行管理时, 需要将此云资源从默认项目迁出 到指定项目。

• 如果用户在 IAM 侧的 Multi-Project 中创建了 Project, 那么在新建资源时, 如果需要与已有的资源 的互通, 需要在选择 Region 时选择 Multi_Project 对应的 Project。

3.2.3 迁出资源

在企业管理页面,选择"企业项目管理"。选择待查看的企业项目,单击操作列【查看资源】。

进入企业项目详情页面,在"资源"页签下可查看该企业项目内资源信息。

1、在列表中选择待迁除资源,单击【迁出】,弹出"迁除资源"页面。

迁出资源

	祆念	♥ 巳后用			创建时间 .	2019-03-08 10:2	0:10 GIALL+09:00
	描述				修改时间	2019-03-08 16:2	6:16 GMT+08:00
	资源	迁出资源				×	
~	区域	单资源迁出支持不同资 业项目;ECS关联迁出	资源同时迁出,其中已关联 仅支持ECS及其关联资源	ECS的EVS、EIP只支持 EVS、EIP同时迁出。	迁入到该关联	ECS所在企	
	产品类	迁出方式 单资源迁出	ECS关联迁出				EIP
	迁	您已选择1个资源,其中1个词	可进行单资源迁出操作。				请输入资源
		资源名称	所属区域	产品类型	资源类型	텓	资源类型
		ecs-9b29	贵州	EVS	磁盘		
		请选择要迁入的企业项目					磁盘
		default	•				弹性云服务器
			确定	取消			32-20090001 天翼云

🛄 说明

迁出操作暂不支持关联操作,如迁出 ECS 不会同时迁出绑定的 EIP、EVS 等,如需迁出关联资源,请选择关联资源一同迁出。

2、确认无误,单击【确定】。资源迁出完成,在迁入企业项目的资源列表中即可查看已迁出的资源。

3.2.4 移除用户组

此处的移除用户组是将企业项目中已添加的用户组移除。

在企业管理页面,选择"企业项目管理"。选择待查看的企业项目,单击操作列【查看用户组】。

进入企业项目详情页面,在"用户组"页签下可查看该企业项目用户组信息。

1、移除支持单个移除和批量移除,操作见下图。

资源	用户组						
添加	u用户组 批量移除						C
	用户组名称	用户数量	关联策略(该	描述	添加时间	操作	
	xz666	1	1	111	2019-01-11 16:35:	设置策略移除	
	yxl	1	1	test	2019-03-19 14:35:	设置策略 移除	

2、点击【移除】/【批量移除】弹出移除确认页面,确认无误后点击【确认】,用户组移除。

	名称 XZ	移除用户组		×	l0d-8f34-05aa76
~	状态・	确定要移版 ^{移除后该用户组}	以下用户组吗? 用户将无法管理该企业项目,如需再次使用,请重新给企业项目添加	响和户组。	09 GMT+08:00 09 GMT+08:00
	资源	用户组名称	描述		
	法加田	xz666	111		
	CI (HCM61	yxl	test		
	☑ 月				H
	x		确定取消		11 16:35: 🔞
	🔽 ухі		1 Lesi	2019-03	s-19 14:35: 🔞

4 常见问题

4.1在什么场景下可以看到所有的企业项目

- 使用主账号登录时,可以查看所有的企业项目信息。
- 使用子账号登录时,如果主账号有对该子账号的全局授权策略,那么子账号将能 看到所有的企业项目信息。

4.2为什么在企业项目管理侧为子账号设置了 EPS Admin 的策略,但该账号不具备添加用户组及设置策略的权 限

对用户组的相关操作依托于统一身份认证服务,因为统一身份认证是全局服务,需要全局策略设置 才能生效。在"企业项目管理 > 用户组"界面绑定的策略的生效范围是当前企业项目,故在用户组 界面的相关操作不生效。

4.3如何获取企业项目 ID

- 通过调用接口获取。
 各云服务可通过 IAM 授权,调用企业项目管理的查询企业项目列表接口获取。
- 通过在企业项目详情页查询获取。操作步骤如下:
 - a. 在企业管理页面,选择"企业项目管理"。
 - b. 单击待查询企业项目名称,进入该企业项目详情页即可查看企业项目 ID。